Association for Information Systems
AIS Electronic Library (AISeL)

ACIS 2004 Proceedings | Australasian (ACIS)

December 2004

Enterprise Security Semantics

Brian Cusack
Auckland University of Technology

Enterprise Security Semantics

Dr Brian Cusack

School of Computer and Information Sciences

Auckland University of Technology

brian.cusack@aut.ac.nz

Abstract

The rise in the use of the Internet and networks for doing online business has altered the ways Information Systems (IS) security is approached and the adoption of enterprise security models. The debate of Information Technology (IT) and business objectives has far-reaching consequences for the design of software and the management of the Business – IT interface. This paper is specifically concerned with conditioning the problem area of information security. The upsurge and continued use of the Internet as a general medium for doing business generates some security problems that have inadequate treatment (and hence conditioning for solutions) within the different worlds of IT and Business. The challenge is being met by the reworking of traditional network security approaches, and the development of new hybrid models.

Keywords

Security, eBusiness, Risk Assurance

INTRODUCTION

The alignment of IT and business objectives is a problematic that invites debate. It is assumed that objectives (measurables) can be treated in some way so that one measure shares contingencies with another. In practice, however, measures are the result of theoretical undertakings that have shaped and produced a measure in keeping with meta-level reflections. Reconciliation at the meta-level remains a problem for effective IT – Business objectives alignment. The key problem area is the differences between IT and business meta-level schema. These may not be easily reconciled by any of the current alignment solutions. Security is generally defined as the protection of assets and information systems security is concerned with the protection of information assets. The problem is further elaborated by considering ambiguity. The semantic coupling of fire and smoke is not sufficient in many contexts, for example, smoke may also be coupled with boy-racer and at the same moment decoupled from fire. Similarly security by definition may not necessarily be coupled with the protection of all possible assets either from an IT perspective or a business perspective, and that semantic decoupling is likely to occur between what business values and what IT values (and visa versa).

eBusiness is an enterprise system that raises all the security issues facing enterprise models. The publicising of eBanking scams that involve impersonation, deception and theft, and other abuses that result in menaces, damage and trust reduction all serve to underwrite public awareness of a problem. eBusiness design and structure materialise from an interlocking layer model, that positions design on the top layer above the layers of infra-structure and info-structure. The lower two layers represent increasing complexity from fundamental IT requirements, such as reliability, security, and data bases, to the middle layer that houses a variety of applications for the co-ordination of customer relationship management, supply chain management, financial control, and so on (Kalatoa & Robinson, 2001, p.106). The layer model separates security considerations into fundamental IT network requirements, customer interaction requirements and managerial requirements. Layering in this view allows the setting of objectives that are negotiated by processes at layer boundaries. A seamless, effective security web that minimises the likelihood of business process vulnerability to unauthorised uses, sabotage, or criminal activity is still a step ahead of current practice. The structural transformation of eBusiness requires the alignment of IT and business objectives for better asset protection.

The use of the internet to do general business, and the integration of technology into enterprise systems (eg. The digital backbone approach (Gates, 1999, p. 15)) has opened systems to violation from uncertainties caught between different ontologies. The adoption of customer-centric business approaches has also introduced the customer as agent and increased the range of possible risks to business assets. Securing information systems is a problem area. In the following sections the problems are further elaborated, attempts to align business and IT objectives reviewed, and the potential for semantic methods to provide solutions foreshadowed.

THE PROBLEM CONTEXT

The debate of IT and Business objectives alignment has illumined a dividing line between the worlds of IT and Business. The debate has tussled back and forth as the different interest groups have carved out respective territories, and substantial literatures have grown in the areas for study. The success of eCommerce as a bridging study between the two worlds developed an IT centric view of technology and business. The initial growth of transaction processing (TPS) culture provided a rational basis on which to extend the techno-logics of IT into the business world. However, the inability of IT to solve business problems and the creation of others has brought resurgence in business centric views as to where IT ought to fit in the business plan. eBusiness was branded to represent the case for business strategic control of all business areas – including IT. The differentiation of eBusiness enterprise modelling from eCommerce (for example, Kalatoa & Robinson, 2001) and the movement towards business control of business objectives (for example, Chaudhury & Kuilboer, 2002) has highlighted ontological problems in the fundamentally different worlds of business, and IT. The shift in emphasis from technologies shaping business purposes and technical developers determining business possibilities, to the retention of control of business processes by the business for business purposes is in the genera of the balanced score card where business activity is a delicate balancing of competing business interests – one only of which is technology (Kaplan and Norton, 1992, 1993, 1996).

The upsurge and continued use of the Internet as a general medium for doing business devolves problems that have inadequate treatment and hence conditioning for solution, within the different worlds of IT and Business. Security is one such problem area. Security in eBusiness information systems (IS) is distributed across different interest groups, all of whom have different expectations for the common sense of trust. In recent literature (for example, Tan & Hunter, 2002) the problem of sense-making in organisations is put as a cognitive problem, divided across end-users, managers and IT professionals, and linked to theory by definitions of schemas, cognitive maps, technological frames, mental models and personal constructs (Tan et.al, 2002, p. 40). In this view common ground for the definition of objects is located by applying the Repertory Grid Technique (RGT), and then by processing the findings using linguistic analysis, factor analysis, and multivariate tools (pp. 49, 50.). In another set of readings the IT Governance literature (for example, Van der Zee, 1999) advocates the setting of finance driven objectives and the distributing of capability to Governance risk management, corporate security, and external assurance audit (Van der Zee, 1999, p.3). The method proposes cascading scorecards that cluster variables consistent with the different stakeholder interests for objective alignment. The alignment is achieved by exercising the Governance capability of risk management and the assumption that sufficient financial performance gain equates with sufficient security.

Objectives alignment is a necessity for secure systems. In situations where the IT and business objective are not aligned each ontology may value objects differently or name them differently and hence disclose assets that ought to be better protected. For example, IT objectives may assure the protection of information at each layer of the network and at each policy level for the system but fail to recognise the business value of clusters or groupings of information. Similarly, the pressures and expectations of business may lead to compromise of disclosure or customer end-user habits compromise authorisation (eg. passwords). The alignment of security objectives is more than setting the standards for interoperation between IT and business and customers. The internet market aggregates the products, services, processes and practices within the industry into which it is attempting to intermediate itself. The information architecture is a marketplace model that captures the richness of marketplaces by modelling elements of business and capturing relationships between them. This is the new internet environment in which IT and business relate and control is negotiated (Alter, 2002, p. 540-541). There are key differences between this environment and the established IT data modelling methods of large-scale enterprise database or datawarehouse organisation. Something new is required to effectively secure large scale eBusiness networks.

SYSTEMS SECURITY

Information systems security is captured in its namesake context of systems. Systems are characterised by complexity, abstract elaboration (modelling), and hypothetical conjecture about change. Systems are generally

defined by what is not known (non-redundancy) and held in the belief that underlying principles (& laws) can be identified for reasoning action. A consequence is that systems are incomplete, caught in change, and that processes (such as systems analysis) provide the linkage of a system to its environment. Security is hence to be effected in a web of interacting complexities and is usually implemented as a trade-off between costs and benefits. Risk is mitigated by cost and the protection of assets optimised against the cost of protection. The concept of total security is hence dispensed and justified sufficiency adopted for asset protection. In Table 1 below six systems modelling principles are taken (from Taylor, 2002, pp. 5-6.) to illustrate the implications for systems security of adopting a systems analysis approach.

Principle	**Definition**	**Security Implications**	**Cost-Benefit Trade-off**
Complexity	Systems are complex structures with many different types of elements that influence each other.	Total security is a myth.	Optimisation of cost and benefits to mitigate risk.
Mutuality	The elements of a system operate at the same time and co-operate or not.	Protected action is filtered by process.	Prioritisation of risks.
Complementarity	Simultaneous exchanges among the elements create subsystems that interact with multiple processes and structures.	Back-box, white-box organisation and protective layers.	Non-redundancy controls risk but can increase semantic vulnerability.
Evolvability	Complex adaptive systems tend to evolve and grow as the opportunity arises as opposed to being designed and implemented to an ideal manner.	New risks arise in an ad hoc fashion. New models and security processes are required.	It is cheaper to over-extend the current model than to create and test new models.
Constructivity	Systems tend to grow and as they do so become bound (inheritance) to their previous configurations while gaining new features.	Ambiguous and alternative objectives may present ineffective protective systems.	The risk of fraud may be discounted against the cost of retaining the previous protective systems.
Reflexivity	Both positive and negative feedback are at work.	The protective system will reflect the internal patterns of use and familiarity arises.	Routine and conditioned agents cost less than pro-active innovation and development.

Table 1. Security Implications of a Systems Analysis Approach

Total and complete network security is a myth, and better viewed as a negotiated condition through which trust is maintained. The key to successful forecasting of systems behaviour is predicting how a system responds to change. The implication for securing information assets is that not only the consequence of a predicted intrusion from the system environment requires assessment but also the consequence (including unforeseen consequences) of trying to mitigate the risk. Security in this sense embraces the intangibility inherent in all systems approaches and accepts an negotiated level of uncertainty. In Table 2 the scope of a systems analysis approach is explored by aligning the phases of implementation with the potential to achieve the objective of securing information assets. The potential of the approach appears comprehensive but a key determinant is the vertical alignment of the objectives. Objectives follow the actions of column two and the system hierarchical model of general (abstractions / goals) to specifics (quantifiables / objectives) is adopted. An objective is hence a measurable and has inherited properties from the abstract layer (Hoffer et.al., 1998, p.191-195).

Phase	Action	Scope
1	Define scope of the problem.	Protecting the information asset.
2	Determine the objectives, constraints, risks, and costs.	The alignment of objectives and the mitigation of risk.
3	Identify alternative course of action.	Multiple mutually exclusive courses of action that will achieve the security objectives.
4	Evaluate the alternatives according to the constraints (feasibility), fixed costs (cost-effectiveness), the ratio of benefits to costs (cost-benefit), or the ratio of benefits to risk (risk-benefit).	Optimisation of asset protection.
5	Recommend an alternative that will meet the needs of a decision-maker but within the system constraints.	The alignment of IT and business objectives for security.

Table 2. The Scope of a Systems Analysis Approach

OTHER APPROACHES

There are many other approaches to securing system that are similar or vary in various ways from the Systems Analysis approach. The following list provides summary of approaches reviewed elsewhere by the author.

- IT Governance Institute professional society (http//:www.itgovernance.org) provides a bridging platform between business objectives and the IT objectives, by focusing on a conception of alignment. In this view an effective risk assurance framework contains a controlled environment that ensures (within an acceptable degree of residual risk) that organisational objectives will be met. The notion of alignment being promoted fits the meta-level framework that defines the problem of IT and business in a triangulated tension of Governance, Security, and Assurance.

- Enterprise modelling presents particular problems for network security that can only be solved by considering the differences between the information systems four key objects, namely; data, technology, organisations, and individuals. Enterprise systems give rise to specific sets of security problems that may have no generality across systems. The key questions to be answered are: What is the enterprise system used for?; What network topology best fits the budget and service requirement ?; How does the organisation perceive and use the technology?; and, What relationship do individuals have with the system? (Taylor, 2002, pp. 15,16).

- Business enterprise systems subsume human, physical and technological subsystems in ways that are specific to the particular business plan. Enterprise wide policies are vulnerable to sub system cultures and variation within communication languages. The pressures of business demands also present security risk in a data range outside of the general considerations of IT security. Motivation and personality analysis approaches are applied to filter the human appetite for risk. The higher a person is positioned in the organisational hierarchy the greater the potential or appetite for risk taking. Training, assurance audit and certification are used for mitigation (Anderson, 2001, p.492).

- Customer centric approaches consider how a customer views the business as a determinate of the quality (if any) relationship they may form with the enterprise. Cox (2001) for example, argued for the presence of at least one or a combination of, power, trust and value in customer transaction. Bigley & Pearce (1998) saw the staged formation of a trust relationship with an eBusiness forming first from cues that satisfy calculative-based trust beliefs, and then if an ongoing relationship takes, from a set of affect-based trust beliefs. Risk perception is a cuing feature in much of the literature reviewed.

- Integrative approaches attempt to partially reconcile differences between discrete layers in an enterprise model by the use of cluster analysis or semantic methods. Integration requires brokerage within the preferred frameworks (modules, blackboxes, applications and so on) and also between the frameworks.

SEMANTIC SOLUTIONS

The power language of business gives two uses of objects; one where a corresponding word is reproduced (brand) and the other where some agents know how to use the word correspondence to effect action (referral).

Similarly in IT the word-object relationship is used in the correspondence way. Earlier in this paper the notion of semantic coupling and decoupling was introduced by example to illustrate the problem area of objectives alignment. The following sections took various approaches for solution to the alignment problem, outlined their strengths and weaknesses and implicated better information systems security for eBusiness with better solutions to the problem. The problem was cast as one of conditioning and one where adequate solutions could not be found within preferred ontologies, such as business or IT. The eBusiness paradigm was introduced as a critical context in which between the frameworks solutions were necessary for sufficient effectiveness. The positioning and casting of the problem has suggested that current approaches fall short of total solutions and that there is further research required for better asset protection, particularly in the eBusiness context.

The mental museum has effective usage (for example, Quine 1968 and so on) as a tool to tease out the nuance of detail necessary for understanding the difficulties of translation and the brokerage between different ontologies. The metaphor starts with the image of a museum in which exhibits are meanings and the words are labels. To switch languages is to change the labels. The problem then arises as to meaning in different languages and the adequacy of the new labels in the "mental museum" of human mental maps (Quine, 1968, p.2). The argument put forward by Quine is that what is lost in simplistic translation of one language to another is determinacy. This is also the problem raised earlier where the translation of IT security objectives into business plans (and visa versa) may result in indeterminacy and ineffective protection. Adequate brokerage of ontologies is complex and problems treated in one or other ontologies may be insufficient to determine likeness of objects or meaning.

The extent to which objectives may be aligned is a problematic that has one solution with an adoption of partial solutions and the rejection of a total security solution. Systems analysis approaches were an example. However, many stakeholders require a higher level of assurance. The IT Governance approach is an example where the court of corporate governance is given the prior right to adjudicate between the worlds of IT and business, and although total security is mitigated, a much higher level of determinacy is gained. Theoretically other solutions are also possible. The inclusion of coherentist methods in information systems epistemology allow for the possibility of criteria based total security solutions. The integrative model outlined above is an example of such an approach.

Semantic unity is as much an ideal as objectives alignment. The translation of meaning from one ontology to another is difficult and fraught with limitations. The solution proposed by the coherentist is that new theories may be adopted when five fundamental tests are satisfied. The tests being:

- Consistency,
- Coherence,
- Comprehensiveness,
- Simplicity, and,
- Potency (or usefulness).

Theories so selected provide holistic justification (ie. from within the theory) and hence the concept, for example, of total security has meaning. Similarly, each element within the theory is evidently coherent in relation to every other element in the network. The method proceeds by the identification of the "best" elements in each competing ontology, and then the positioning of the preferred elements into a new relational web. The positioning of elements provides structure, the overall structure a theory, and the theory may be revised by testing in practice. Each element added or subtracted from a structure is tested for consistency, coherence, comprehensiveness, simplicity and usefulness (Quine, 1976).

CONCLUSION

The eBusiness paradigm presents a new set of challenges for enterprise modelling, and for coherent and consistent methods that can deliver stability for decision-making within the new framework. In this paper the concern of IT and business objective alignment has been discussed in order to evaluate the relative strengths and weaknesses of different approaches for protecting assets in the eBusiness context. Semantic methods offer an alternative solution to the alignment problem and propose an outcome closer to total protection. The tension of IT requirements and business demands requires between the frames adjudication. The move to customer centred enterprise development provides a momentary solution between the divide but it also raises a significant challenge to both IT and Business – that of negotiating a seamless, effective security web to minimises the likelihood of business process vulnerability in unauthorised uses, sabotage, or criminal activity. The reworking of the issue views negotiation between the frameworks as being critical to progress in eBusiness asset protection. Imposition by force of alignment mandates or abdication of responsibility in cultural constructs falls short of achieving the level of confidence a caring customer may trust. Considerable trust has been lost through the current use of IT and Business models.

The ontologies of IT and Business are different, therefore objects are defined differently and meanings ambiguous. The security architect has to work with these differences and broker a new platform on which the rules, resource designations, and schemas deliver secure functionality. Achieving semantic unity with disparate ontologies can be gained by appealing to the methods of coherentist philosophers and the recasting of assurance problems into new and coherent meta schema for knowledge. This work is in the abstract layer and has many possible solutions.

REFERENCES

Alter, S. (2002) Information Systems; The Foundations of eBusiness (4th Edition), Prentice Hall, New Jersey.

Anderson, R. (2001) Security Engineering, Wiley, New York.

Bigley, G. & Pearce, J. (1998) Straining for Shared Meaning in Organisational Science: Problems of Trust and Distrust, *Academy of Management Review*, 23(3), 405-421.

Brand, K., Boonen, H. (2004), *IT Governance a Pocket Guide Based on COBIT*, Inform, Netherlands.

Chaudhury, A. & Kuilboer, J. (2002) eBusiness and eCommerce Infrastructure, McGraw Hill, New York.

Cox, A. (2001) Understanding buyer and supplier power: A framework for procurement and supply competence, *Journal of Supply Chain Management: An International Journal*, 4(4), 8-15.

Gates, B. (1999) *Business at the Speed of Thought*, Time Warner, New York.

Gremberggen, (2002) The Balanced Score Card, *IT Governance Institute*.

Grubbler, T. (1993) A Translation Approach to Portable Ontologies, *Knowledge Acquition*, 5(2), 199-220.

Hoffer, J, George, J., Valacich, J. (1998) *Modern Systems Analysis & Design*, Addison-Wesley, New York.

Kalakota, R. & Robinson, M. (2001) e-Business Road Map for Success (2nd Ed.), Addison-Wesley, New York.

Kaplan, R. & Norton, D. (1992) The Balanced Score Card: Measures that drive, *Harvard Business Review*, Jan.-Feb. 71-79.

Kaplan, R. & Norton, D. (1993) Putting the Balanced score Card to Work, *Harvard Business Review*, Sept. – Oct. 134-142.

Kaplan, R. & Norton, D. (1996) Using the Balanced Score Card as a Strategic Management System, *Harvard Business Review*, Jan. – Feb. 75-85.

Lee, M. & Turban, E. (2001), A trust Model for Consumer Internet Shopping, *International Journal of Electronic Commerce*, 6(1), 75-91.

Mitchelle, V. (1999) Consumer Perceived Risk: Conceptualisations and Models, *European Journal of Marketing*, 33(1/2), 163-195.

Quine, W. (1976), *Mind and Language*, Oxford University Press, Oxford.

Quine, W. (1968),Ontological Relativity, *The Journal of Philosophy*, 65(7), 1-16.

Shleifer, A. & Vishny, R. (1997) A Survey of Corporate Governance, *The Journal of Finance*, June, 737-783.

Tan, F. & Hunter, M. (2002) The Repertory Grid Technique: A Method for the Study of Cognition in Information Systems, *MIS Quarterly*, 26(1), 39-57.

Taylor, T. (2002) *Security*, Sybex, California.

Van der Zee, J. (1999) Alignment is not enough: Integrating Business and IT Management with the Balanced Score Card, *Proceedings of the Conference on IT and the Balanced Score Card*, 1-21.

COPYRITE